CYBERCRIME NEWS

ISSUE 13 • FEBRUARY 2025

RANSOMWARE: A GROWING THREAT TO BUSINESSES

RANSOMWARE ATTACKS ARE ONE OF THE MOST SEVERE CYBER THREATS BUSINESSES FACE TODAY.

AT DORSET POLICE, WE HAVE SEEN A RISE IN RANSOMWARE CASES TARGETING LOCAL BUSINESSES, HIGHLIGHTING THE IMPORTANCE OF STAYING VIGILANT AGAINST THIS THREAT.

This malicious software locks your files and systems until a ransom is paid, often in cryptocurrency. The consequences of a ransomware attack can be devastating, resulting in financial loss, operational disruption, and reputational damage.

Ransomware has become a very lucrative business model for cyber criminals, with many people seeing no option but to pay. Our advice will always remain the same - DO NOT PAY.

PREVENTING RANSOMWARE: PRACTICAL STEPS

1 BACKUP YOUR DATA

- Regularly backup your files and ensure backups are stored offline.
- Backups should be kept on a separate device or location not connected to your main network, such as an external hard drive or a secure cloud service. This prevents ransomware from encrypting your backups along with your primary data.
- Test your backups regularly to ensure they work and include all critical files. Consider implementing a 3-2-1 backup strategy: Keep three copies of your data, on two different media types, with one copy stored offsite.
- Additionally, plan the timing of your backups carefully. The data in your backups represents the point in time to which you can revert to if your systems become compromised. Frequent backups reduce the risk of significant data loss.

MORE...

HOW DOES RANSOMWARE WORK?

RANSOMWARE TYPICALLY INVOLVES A PREDICTABLE ATTACK LIFECYCLE:

1. INFECTION

Computer systems are infiltrated using phishing emails, malicious links, or compromised software.

2. ENCRYPTION

Once inside, the ransomware encrypts your critical files, rendering them inaccessible.

3. RANSOM DEMAND

The attackers then demand payment, often threatening to leak your data if the ransom is not paid.

4. POTENTIAL DATA LEAK

Even if the ransom is paid, there is no guarantee your data will be returned or that is hasn't been compromised.

DORSET POLICE & CRIME COMMISSIONER DAVID SIDWICK

PRODUCED BY DORSET OPCC AND DORSET POLICE

DORSET POLICE

2 KEEP SYSTEMS UPDATED

Ensure your devices and systems are kept up to date. Software and hardware providers release updates in the form of patches. Patches often contain important security related fixes. Unpatched software and hardware are attractive to cybercriminals, and the release of an update makes them aware there is something to potentially exploit. This is why it is important to apply patches as soon as they become available. For organisations with large networks, consider a controlled release of each update.

3 BE WARY OF UNSOLICITED EMAILS, LINKS, & ATTACHMENTS

Email is by far the most common way in which malware is delivered to our systems, being used in approximately 95% of attacks. Be mindful if you receive an email you weren't expecting, even if it is from a trusted contact.

If you receive an unexpected email, take time to verify it with the sender. If it is a trusted contact, consider contacting them by phone, SMS, or another communication channel aside from email. If you cannot confirm the origin of the attachment, be very cautious opening it.

WHAT TO DO IF YOU DO FALL VICTIM

If you suspect a ransomware attack:

- **Disconnect affected devices:** Isolate impaired systems to prevent malware from spreading.
- **Report the incident:** Contact **Dorset Police** on **101**, or **Action Fraud** on **0300 123 2040** and report the incident.
- **Do not pay the ransom:** Payment does not guarantee data recovery and may encourage further attacks.
- Visit **www.nomoreransom.org/en/index.html** for help, advice, and decryption tools for some strains of ransomware.

REPORTING CYBER CRIME

If you fall victim to fraud or cyber crime, you can report this to Action Fraud by visiting www.actionfraud.police.uk or by calling 0300 123 2040.

If you have received an email that you're not sure about, you can report this to the **National Cyber Security Centres Suspicious Email Reporting Service (SERS)**. Simply forward the email to **report@phishing.gov.uk**.

The SERS automatically analyses suspicious emails and, if it considers it to be malicious, can take steps to have email accounts and associated websites closed down, meaning each report can really make a difference.

DORSET POLICE

Dorset Police
Force Headquarters
Winfrith, Dorchester
Dorset DT2 8DZ

E cybercrimeprevention@dorset.pnn.police.uk
www.dorset.police.uk

DORSET POLICE & CRIME COMMISSIONER DAVID SIDWICK

Office of the Dorset Police & Crime Commissioner
Force Headquarters
Winfrith, Dorchester
Dorset DT2 8DZ

T 01202 229084
E pcc@dorset.pnn.police.uk
www.dorset.pcc.police.uk